QUICK START MANAGEMENT GUIDE FOR VOTING SYSTEM SECURITY

The Quick Start Management Guide for Voting System Security is a snapshot of processes and procedures for local election administrators to use when implementing security measures for their voting systems. It is not intended to be a comprehensive security tool but a guide that highlights priority items essential to securing a voting system. A comprehensive set of Management Guidelines is under development and will be released in modules in 2007 and 2008.

Software Security

- Ensure that the software installed on the voting system is the exact version that has been certified by your State, the National Association of State Election Directors (NASED), and/or the Election Assistance Commission's Voting System Testing and Certification Program. If you have any reason to suspect that your voting system software has been compromised, reinstall the voting system software by using a copy of the software obtained directly from your State Election Office or the laboratory that tested the voting system.

- Do not allow any software on your vote-tabulating computer except the voting system software itself. Specifically, do not allow office automation software, such as Microsoft® Word, PowerPoint, and Excel, or networking software, such as e-mail and network browsers.

- Verify that your voting system is not connected to any network outside the direct control of the Election Office. All unused connections on the voting systems should be sealed, including universal serial bus (USB), parallel, and other ports.

- Familiarize yourself with the content of the audit logs on your voting system and learn to print them.

- Consider any results transmitted electronically from the precinct to the central office to be unofficial and verify them against the results contained on the media that are physically transported to the central office. Example: *Reload all voting machine memory cards into the central tabulation computer to validate any unofficial results that are transmitted via modem to your office on election night.*

Policies and Procedures

- Develop a specific procedure for monitoring each person who has access to your voting system, including your Election Office staff, vendor personnel, and visitors to your office.

- Require positive identification of each person who requests access to the voting system. Keep a log of everyone who accesses the voting system. This log should include the person's name, the purpose of the access, and the date and time the access begins, and the time the access ends. The entries in this log must be complete. Example: *"System*

Maintenance" is not an acceptable entry. The entry should state who accessed the system, exactly what maintenance was performed and why it was necessary, when the maintenance work began, and when it ended.

- Issue passwords to staff that will allow them to perform only authorized functions on the voting system. It is highly recommended that members of the election staff work in pairs whenever possible. This procedure will greatly reduce the potential for accidental errors and virtually eliminate any opportunity for deliberate mischief or fraud by a rogue employee.

- Control the access of vendor personnel to your system until you are absolutely certain that any change, upgrade, or maintenance that they intend to perform has already been approved by the Federal and/or your State certification process. It is essential that the vendor never be allowed access to the voting system without a member of the Election Office staff present. In this context, a non-vendor consultant working under contract with the Election Office is considered to be a member of the Election Office staff; however, consultants should be monitored as closely as vendor personnel are.

Password Maintenance

- Designate someone in the Election Office as the Password Administrator. This person should be either the Chief Election Officer or a senior member of the Election Office staff. The Password Administrator performs the following duties:

  1. Issues passwords.
  2. Maintains a master list of all passwords issued.
  3. Reissues all passwords periodically.
  4. Monitors password usage.

  A printed copy of the master list of passwords should be kept by the Password Administrator in a safe and secure place at all times and should only be used in the event of an office emergency.

- Never issue a system password to anyone (including vendor personnel) other than an employee of the Election Office.

Physical Security

- Engage county and municipal information technology staff and/or local community college or technical school staff to help conduct a security review and establish and implement applicable election management system security measures.

- Create or update appropriate procedures to ensure that absentee and emergency ballot blank paper stocks are controlled at all times.

- Develop physical security procedures and safeguards to document the controlled physical access to voting systems and the facility where the systems are stored. Document all security-related repairs and modifications to the physical components of the facility where voting systems are stored (e.g., walls, doors, locks, cameras, alarm systems).

- Review Election Office work areas to ensure that office space is appropriately isolated and that undetected access by unauthorized individuals is not possible. Review voting equipment storage and work areas to ensure that only authorized personnel have access to them.

- Maintain a list of personnel who have keys to Election Office work areas and voting equipment storage to ensure that all keys are accounted for and only authorized personnel have keys.

Develop procedures and policies requiring that keys or combination locks be changed for each election cycle.

- Develop chain-of-custody procedures, use tamper-evident seals, and implement inventory control/asset management processes to ensure that voting units and associated equipment are properly and securely controlled and accounted for at all times throughout the election administration process.

- Review all election audit trail checklists to ensure that they incorporate two-person integrity security measures, such as dual signoff..

Personnel Security

- Establish qualification guidelines for choosing the person(s) who will operate and administer the voting system and perform background checks on election officials who are authorized to define and configure elections and maintain voting devices.

- Allow only authorized personnel to physically access the voting system. For tracking purposes, issue each staff member a unique entry code.

- Require staff members to wear identification badges at all times. When visitors, vendors, maintenance personnel, and other non-staff individuals enter Election Office work areas, log their entry and exit dates and times, record the purpose of their visit, and issue them numbered temporary identification badges.

- At each polling place establish the number of personnel needed and identify their duties, maintain separation of duties for poll managers, incorporate two-person integrity security measures, and provide adequate security for election equipment at all times. Establish policies and/or procedures for visitors and observers in the polling place.

Securing the Voting Devices During Preparation and Transport to the Precinct

- Secure the voting devices with tamper-proof numbered seals and record the serial numbers for each device. These numbers should be verified during setup at the precinct.

- Develop an operational plan that defines that the voting devices that will be delivered and that describes where and when they will be delivered and who will deliver them.

Securing the Voting Devices During In-Person Absentee and/or Early Voting

- Use the same procedures to prepare, test, deliver, and set up in-person absentee and/or voting devices as those used to prepare, test, deliver and set up voting devices that are used in the polling places on Election Day.

- Place voting storage media in the same voting devices each morning and remove the media each night.

- Close, seal, and secure the voting devices at the end of each day. Secure the voting storage media each night in a tamper-proof location, preferably within the Election Office.

- Verify the numbers on all protective seals and public counters before the voting devices are used for voting the next morning.

Securing the Voting Devices on Election Day

- Require the poll manager to verify and sign off on the serial numbers of all voting devices and necessary election supplies (e.g., ballot activation devices, administrator devices, communication equipment, closing seals).

- Require the poll manager to verify the numbers of all seals and/or tamper-resistant tape on all voting devices and inspect the voting devices for any evidence of tampering. Require the poll manager and all poll workers to use a checklist to verify that all opening procedures were followed and then sign off on that checklist.

- Control access to the voting device's power control, counter controls, and election results storage media. The polling place should be arranged so that the exterior of the voting device is in plain view of the poll manager(s) at all times.

- Allow only poll managers and registered voters in the voting device area. A voter should not be allowed to enter this area until a voting device is available for his or her use. The poll manager should maintain control of administrator and ballot activation devices.

- Encourage poll managers to periodically verify the number of voters processed against the number of votes recorded (via public counter) on the voting devices and to compare that number with the total number of signatures recorded in the poll book.

Securing the Voting Devices During Tabulation

- Use a numbered, sealed pouch to transport storage media from the polling place to the local Election Office or designated collection point.

- Establish procedures to securely transport election results from optical scanners to vote-tabulating computers if the optical scanners are not located in the same location as where vote tabulation takes place.

- Verify the results transmitted by modem from the precincts to the central Election Office by performing a separate count of the election result storage media containing the original votes cast.

- Allow only authorized election officials in the tabulation equipment room.

- Consider using uniformed security or police officers to secure the ballot room and/or voting equipment during tabulation.

Securing the Voting Devices During Storage and Post-Election

- Verify that all voting devices are returned to storage, confirm that the devices have not been tampered with during transport, and sign off on the receipt of the voting devices.

- Maintain an inventory of election materials, including voting devices, administrator and ballot activation devices, seal envelopes, voter registration (poll) lists, election result tapes and printouts, field supervisors' reports, poll workers' daily logs, reconciliation reports, audit data, and other items.